## REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion is respectfully requested.

Claims 1-10 are pending in the application. Claims 9 and 10 are newly added by the present amendment. Support for new Claims 9 and 10 can be found in the original specification, claims and drawings.[1] Thus, no new matter is presented.

In the outstanding Official Action, Claims 1 and 4-6 were rejected under 35 U.S.C. § 102(b) as anticipated by Ishiguro et al. (U.S. Patent No. 5,883,958, hereinafter "Ishiguro"); and Claims 2, 3, 7 and 8 are rejected under 35 U.S.C. § 103(a) as unpatentable over Ishiguro in view of Yagawa et al. (U.S. Patent No. 6,751,598, hereinafter "Yagawa").

The outstanding Official Action asserts that Ishiguro teaches all the elements of independent Claim 1. Applicants respectfully traverse this rejection.

Briefly recapitulating, the present invention provides a system and method that prevents data from being manipulated in an unauthorized manner. In an exemplary, non-limiting embodiment, encrypted digital data is downloaded with management information including various parameters relating to the downloaded data. Among other parameters, the management information also includes usage rule parameters restricting the transfer and use of the digital data.[2] These parameters form the basis for a calculated MAC value generated each time an "operation" is performed on the digital medium. It should also be noted that this MAC value includes updatable information which is modified based on an "operation" that may be performed on the digital data.

The MAC value is generated using the encryption key for the content, as well as the above-noted updatable calculation information reflecting the current status of the digital

---

[1] Specification at Figs. 4 and 9.
[2] Specification at pages 8-9.

data.[3] Each time an operation is initiated on the digital file, the MAC value currently stored

in memory is compared to a newly calculated MAC value generated in response to the

initiation of the operation. If the result of the comparison shows that the two MAC values

differ, then an unauthorized operation was performed on the data and use of the digital data is

restricted.

Specifically, Claim 1 recites, *inter alia*, an information processing apparatus,

comprising:

> ...calculation means for ***performing a predetermined calculation on the basis of said encryption key and said calculation information***, said calculation information including updatable information which is updated upon execution of a predetermined operation performed on said content data...
> control means for ***comparing the result of the calculation performed by said calculation means*** with a previous calculation result stored in memory means and controlling use of said content data stored in said storage means in accordance with the result of the comparison.

Turning to the applied reference, Ishiguro describes a method and device for tamper

resistant video data playback.[4] Specifically, Ishiguro describes that multiple sets of public

keys, used to decrypt the video data, are retrieved from the DVD-ROM (2).[5] Each public key

includes a corresponding "flag" indicating whether the key is valid. A controller (20) of the

disc drive extracts the public key and associated flag relevant to the ID received from the

controller (30).[6] The controller (20) then verifies the validity of the flag of the public key.

Once the key is validated, a challenge is calculated by the controller using the key, a prime

number and other variables to confirm that the controller has authorization to access the

data.[7]

In contrast, Claim 1 recites that calculations are performed on the basis of the

encryption key and calculation information (which is updatable based on an operation) and

---

[3] Id. at p. 37, lines 15-21.
[4] Ishiguro at Abstract.
[5] Id. at col. 3, lines 54-65.
[6] Id. at col. 4, lines 6-15.
[7] Id.

that a comparison is performed between the result of this calculation and stored calculation information. In addressing the claimed "calculation information" the outstanding Official Action relies on col. 3, lines 54-65 of Ishiguro and states that "the flag indicating whether the public key is valid/invalid serves as calculation information".[8] However, the flag indicating the validity of the public key could not possibly correspond to the calculation information, as recited in Claim 1, because the validity flag is not used in a *calculation* with an encryption key, the results of the calculation being compared with other calculation information to control the use of the content data.

Specifically, Ishiguro describes that validity flags correspond to each of the public keys in the DVD-ROM device and before a key is used, it is analyzed to determine whether it can be used to decode the information stored on the DVD-ROM device (is valid).[9] The outstanding Official Action relies on "formulas 1, 2, or 3" of col. 4, lines 30-55 of Ishiguro in addressing the claimed feature of a "calculation means which performs a predetermined calculation on the basis of the encryption key and the calculation information", again relying on the flag as the calculation information. However, as is clearly shown in col. 4, lines 28-55 of Ishiguro, none of the formulas include a variable indicating that the flag is used in the calculation.

Therefore, Ishiguro fails to teach or suggest a calculation means for performing a predetermined calculation on the basis of said encryption key and said calculation information, as recited in Claim 1.

Further, Claim 1 recites a control means for comparing the results of the calculation performed by the calculation means with the previous calculation result stored in said memory means and controlling the use of the content data stored in the storage means in accordance with the result of the comparison. In addressing this claimed feature, the

---

[8] Outstanding Official Action at page 3, second paragraph.
[9] Id. at col. 4, lines 6-23.

outstanding Official Action relies on col. 4, line 43 – col. 5, line 15 of Ishiguro. However, as stated above, the calculations performed in the cited portion of Ishiguro do not include the flag indicating the validity of the public key, which is cited in the outstanding Official Action as corresponding to the updatable calculation information as recited in Claim 1. Instead, Ishiguro performs calculations at both the controller and the decoder which include the key and a random number and a prime number, and these calculations are exchanged to generate a digital signature allowing the user to gain access to a session key. However, none of these calculations involve the use of a flag indicating the validity of a public key or any other data which is updatable upon the execution of a predetermined operation performed on the content data, as recited in Claim 1.

Accordingly, Applicant respectfully requests the rejection of Claim 1 under 35 U.S.C. § 102(b) be withdrawn. For substantially the same reasons as given with respect to Claim 1, it is also submitted that Claims 4, 5 and 6 patentably define over Ishiguro. As Claims 3 and 8 depend from Claims 1 and 7, respectively, it is submitted that these claims also patentably define over Ishiguro, for at least the reasons cited above.

Claims 2, 3, 7 and 8 were rejected under 35 U.S.C. § 103(a) as discussed above, Ishiguro fails to teach or suggest the above-noted features recited in Claim 1. Likewise, Yagawa fails to remedy this deficiency, and therefore none of the cited references, alone or in combination, teach or suggest Applicants' Claims 2, 3, 7 and 8 which include the above-noted feature by virtue of dependency. Therefore, the Official Action does not provide a *prima facie* case of obviousness with regard to any of these claims.

Accordingly, Applicants respectfully requests the rejection of Claims 2, 3, 7 and 8 under 35 U.S.C. § 103 be withdrawn.

Further, new Claims 9 and 10 are added which recite subject matter which is similar to that recited in amended Claim 1, but further clarify that the calculated value is a has value,

and the calculation performed to obtain the hash value involves a part of the content data and

a sequentially incremented number which is incremented based on an operation performed on

the data.

As stated above, <u>Ishiguro</u> fails to teach or suggest using an updatable number in a

calculation to control access to the content data, as recited in new Claims 9 and 10.

Accordingly, Applicants respectfully submit that new Claims 9 and 10 patentably

define over the applied references for at least the reasons discussed above.

Consequently, in view of the present Amendment and in light of the foregoing

comments, it is respectfully submitted that the invention defined by Claims 1-10 is patentably

distinguishing over the applied references. The present application is therefore believed to be

in condition for formal allowance and an early and favorable reconsideration of the

application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Customer Number

**22850**

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

I:\ATTY\ATH\PROSECUTION\20'S\203742-US\203742 AM 7.14.05.DOC

11